ISSEP®

Information Systems Security Engineering Professional

ISC2 Certification

Certification **Exam Outline**

Effective Date: August 1, 2025

ISC2

ISSEP Information Systems Security Engineering Professional
ISC2 Certification

About ISSEP

The Information Systems Security Engineering Professional (ISSEP) is a security leader who specializes in the practical application of systems engineering principles and processes to develop secure systems. An ISSEP analyzes organizational needs, defines security requirements, designs security architectures, develops secure designs, implements system security, and supports system security assessment and authorization for government and industry.

The broad spectrum of topics included in the ISSEP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of security engineering. Successful candidates are competent in the following five domains:

- Systems Security Engineering Foundations
- Risk Management
- Security Planning and Engineering
- Systems Security Implementation, Verification and Validation
- Secure Operations, Change Management and Disposal

Experience Requirements

Candidates must be a CISSP in good standing and have two years' cumulative, full-time experience in one or more of the five domains of the current ISSEP outline.

Or

Candidates must have a minimum of seven years' cumulative, full-time experience in two or more of the domains of the current ISSEP outline. Earning a post-secondary degree (bachelor's or master's) in computer science, information technology (IT) or related fields or an additional credential from the ISC2 approved list may satisfy one year of the required experience. Part-time work and internships may also count towards the experience requirement.

Accreditation

ISSEP is in compliance with the stringent requirements of the ANSI National Accreditation Board (ANAB) ISO/IEC Standard 17024.

Job Task Analysis (JTA)

ISC2 has an obligation to its membership to maintain the relevancy of the ISSEP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by security professionals who are engaged in the profession defined by the ISSEP. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of today's practicing information security professionals.

ISSEP Examination Information

Length of exam	3 hours
Number of items	125
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam availability	English
Testing center	Pearson VUE Testing Center

ISSEP Examination Weights

Domains	Weight
1. Systems Security Engineering Foundations	24%
2. Risk Management	20%
3. Security Planning and Engineering	22%
4. Systems Security Implementation, Verification, and Validation	20%
5. Secure Operations, Change Management and Disposal	14%
Total:	**100%**

Domain 1:
Systems Security Engineering Foundations

1.1 Apply systems security engineering fundamentals

» Systems security engineering trust concepts and hierarchies

» Relationships between systems and security engineering processes

» Structural security design principles (e.g., National Institute of Standards and Technology (NIST) engineering framework, International Organization for Standardization (IS0) 27001)

1.2 Execute systems security engineering processes (e.g., hardware, software, data)

» Organizational security authorities (e.g., internal, external)

» System security governance and compliance (e.g., laws, regulations, standards)

» Design concepts (e.g., open, proprietary, modular)

1.3 Integrate with system development methodology

» Security tasks and activities

» Security requirements verification throughout the process

» Assurance methods (e.g., software, hardware, virtual, cloud)

» Models (e.g., System Development Life Cycle (SDLC), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24641:2023, Model based systems engineering)

1.4 Perform technical management

» Project management processes participation

» Configuration management (CM) processes

» Information management processes

» Measurement processes

» Quality assurance (QA) processes

» Security process automation solution evaluations

Domain 1:
Systems Security Engineering Foundations

1.5 Participate in the technology procurement management

» Security requirements for acquisitions

» Selection process

» Supply chain risk management (SCRM)

» Review security related contractual deliverables (e.g., hardware, software, services, documentation)

1.6 Resource Analysis (e.g., Cost estimation, personnel costs, probabilities and statistics (Monte Carlo))

» Cost estimation

» Personnel costs

» Probabilities and statistics (Monte Carlo method, mean time between failures (MTBF), Maximum Tolerable Downtime (MTD), mean time to failure (MTTF), mean time to repair (MTTR), mean time to recovery (MTTR))

Domain 2:
Risk Management

2.1 Apply security risk management principles

» Security risk management alignment with enterprise risk management

» Risk management integration throughout the lifecycle

2.2 Manage risk to system

» Establish risk context

» Identify system security risks (e.g., threats, events, vulnerabilities, impact)

» Perform inherent risk analysis

» Perform risk evaluation

» Monitoring and evaluate changes to risk posture (e.g., residual, changed, new)

» Documenting risk posture (e.g., findings, decisions)

2.3 Manage risk to operations

» Establish risk context

» Identify system security risks (e.g., threats, events, vulnerabilities, impact)

» Perform inherent risk analysis

» Perform risk evaluation

» Monitoring and evaluate changes to risk posture (e.g., residual, changed, new)

» Documenting risk posture (e.g., findings, decisions)

Domain 3:
Security Planning and Engineering

3.1 Analyze organizational and operational environment

» Capture stakeholder requirements
» Identify roles and responsibilities
» Identify relevant constraints and assumptions
» Prepare security validation plan

3.2 Apply system security principles

» Resiliency methods (e.g., redundancy, component diversity/disparity)
» Layered security concepts (e.g., defense-in-depth, Zero Trust, secure-by-default)
» Fail-safe defaults (e.g., fail open, fail secure, fail closed)
» Single points of failure
» Least privilege
» Economy of mechanism
» Separation of interfaces, functions, services, and roles
» Automation (e.g., threat response, SecDevOps, emerging technologies)
» Software assurance
» Data security

3.3 Develop system requirements

» Develop system security context
» Identify functions within the system and security concept of operations
» Document system security requirements baseline
» Analyze system security requirements

3.4 Create system security design

» Develop functional analysis and allocation
» Develop system security design components
» Maintain traceability between specified design and system requirements
» Perform trade-off studies
» Validate design

Domain 4:
Systems Security Implementation, Verification and Validation

4.1 Implement and integrate security solutions

- Perform system security implementation and integration
- Support on-going system security activities (e.g., Continuous Integration and Continuous Delivery (CI/CD), DevSecOps)

4.2 Verify successful implementation

- Develop security test plans
- Support system security verification
- Review and update risk analysis
- Document stakeholder acceptance in system implementation

Domain 5:
Secure Operations, Change Management and Disposal

5.1 Develop secure operations plan

- Identify roles, responsibilities, and requirements for system security personnel conducting operations
- Specify requirements for security related event reporting

5.2 Support secure operations

- Design continuous monitoring functionality (e.g., personnel, processes, technology)
- Support the incident response process
- Develop secure maintenance procedures

5.3 Participate in change management

- Participate in change reviews
- Assess change impact
- Perform verification and validation of changes
- Update risk assessment documentation

5.4 Participate in the disposal process

- Identify disposal security requirements
- Develop secure disposal plan
- Develop decommissioning and disposal procedures
- Audit results of the decommissioning and disposal process
- Implement data retention policies

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at **www.ISC2.org/certifications/references**.

Examination Policies and Procedures

ISC2 recommends that ISSEP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at **www.ISC2.org/Register-for-Exam**.

Legal Info

For any questions related to **ISC2's policies**, please contact the ISC2 Legal Department at legal@isc2.org.

Any Questions?

Contact ISC2 Candidate Services in your region:

Americas Tel: +1.866.331.ISC2 (4722), press 1
Email: membersupport@isc2.org

Asia-Pacific Tel: +(852) 5803-5662
Email: isc2asia@isc2.org

Europe, Middle East and Africa Tel: +44 (0)203-960-7800
Email: info-emea@isc2.org

ISC2